

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X

UNITED STATES OF AMERICA :

-v.- : 24 Cr. 424 (JGK)

HDR GLOBAL TRADING LIMITED, :
a/k/a/ "BitMEX," :

Defendant. :
:

-----X

THE GOVERNMENT'S SENTENCING MEMORANDUM

DAMIAN WILLIAMS
United States Attorney
Southern District of New York

Jessica Greenwood
Thane Rehn
Assistant United States Attorneys
Southern District of New York
- Of Counsel -

TABLE OF CONTENTS

PRELIMINARY STATEMENT	1
FACTUAL BACKGROUND.....	2
PROCEDURAL HISTORY.....	8
DISCUSSION	10
I. Application of the Sentencing Guidelines	10
A. Step One: Calculating the Gain from the Offense	10
1. A Conservative Estimate of the Company’s Gain is \$128 Million.....	10
2.The Government Did Not Stipulate to Any Different Gain Amount....	14
B.Step Two: The Culpability Score and Multiplier	16
C.Steps Three and Four: Disgorgement and Offset	18
II. The Nature, Circumstances, and Seriousness of the Offense	19
III. A Substantial Financial Penalty is Required to Afford General Deterrence and to Promote Respect for the Law	22
IV. Comparator Cases	25
CONCLUSION.....	26

The Government respectfully submits this memorandum in advance of the sentencing of the corporate defendant HDR Global Trading Limited, a/k/a “BitMEX,” presently scheduled for October 7, 2024, and in response to the defendant’s sentencing memorandum dated September 6, 2024 (“Def. Mem.”).

PRELIMINARY STATEMENT

From September 2015 to September 2020, HDR Global Trading Limited, a/k/a “BitMEX,” (“BitMEX” or the “Company”) willfully violated the Bank Secrecy Act by operating in the United States without an adequate anti-money laundering program, even ignoring the basic requirement to obtain identification information from its customers. The implementation of such programs by financial institutions is vital to the interests of the United States because such programs help combat money laundering and terrorist financing, deter and detect fraud, and require the institutions to report suspicious activities to help law enforcement authorities identify serious crimes. But instead of complying with the law, BitMEX willfully flouted it, knowingly operated in the United States by surreptitiously serving U.S. customers and maintaining employees and offices in this country, without any such program, and did so understanding well the consequences. The pecuniary benefits were immense: the lack of an AML program while operating in the United States allowed BitMEX to grow into a wildly profitable business. The company processed trillions of dollars of transactions for its anonymous customers, which yielded more than \$1.3 billion in revenue to the Company over the course of just a few years, all while its individual founders grew in power and influence in the cryptocurrency industry. Due to its deliberate choice not to have any AML policy, BitMEX processed hundreds of millions of dollars in illegal or suspicious transactions, openly traded with individuals in sanctioned jurisdictions, and, at times, knowingly allowed criminal actors to transfer funds through its platform.

Corporations cannot be imprisoned, but they can and should be sentenced to financial penalties. As with individual defendants, the proper starting place for considering the appropriate fine is the United States Sentencing Guidelines. Although there are strong arguments in favor of a much higher Guidelines range, the Government ultimately submits that the applicable Guidelines range is a fine of \$223,416,000 to \$428,832,000. As described below, all the relevant factors weigh in favor of a sentence at the high end of this range, so the Government submits that a fine in the range of \$428 million is warranted in this case. BitMEX’s proposal that it pay no further financial penalties would be wholly inadequate to serve the ends of sentencing set forth in Section 3553(a). The fact that the individual founders already paid monetary penalties to address their own individual criminal misconduct and that the company undertook remedial measures after they received scrutiny from U.S. authorities and the founders were indicted is simply not an adequate basis to impose no additional financial penalty. Such a sentence would send exactly the wrong message to corporate defendants.

FACTUAL BACKGROUND

BitMEX was founded in 2014 by Arthur Hayes, Ben Delo, and Sam Reed (the “Founders”). From its launch, BitMEX operated as a trading platform that offered financial derivatives settled in Bitcoin. (Hayes PSR ¶ 14).¹ Greg Dwyer was the first-non Founder employee of BitMEX.

During the charged time period, among other products, BitMEX allowed its customers to buy and sell futures contracts and swaps tied to the price of Bitcoin and other cryptocurrencies, and accepted Bitcoin both to margin and to guarantee actual and potential trades. BitMEX offered and sold these commodity derivatives to U.S. customers, including “retail” customers. BitMEX also operated a substantial portion of its business in the United States, including by maintaining

¹ The Probation Office has not yet finalized the PSR for BitMEX, so the Government’s citations herein are primarily to the PSRs for the Founders, which this Court has previously adopted.

offices in New York and San Francisco from at least spring 2017 through October 2020. Additionally, Reed, who served as the Company's Chief Technology Officer and had substantial roles developing BitMEX's technology, worked for the Company while in the United States throughout the relevant period.

Because it conducted business and maintained offices in the United States, and because it accepted orders from and otherwise dealt in leveraged commodities derivatives with U.S. customers, BitMEX was a futures commission merchant ("FCM") required under the Commodity Exchange Act ("CEA") to register as such with the United States Commodity Futures Trading Commission (the "CFTC"). Based on its FCM status, BitMEX was also required to implement anti-money laundering ("AML") and know-your-customer ("KYC") controls under CFTC rules and the BSA, which apply to registered and unregistered FCMs.

BitMEX and its executives were aware of the applicable regulations, yet they deliberately structured BitMEX so that it did not implement an AML or KYC program. Indeed, when the Company was founded in 2014, the Founders incorporated in the Seychelles specifically because the country "has no clarity on Bitcoin," and chose to transact with its customers exclusively in Bitcoin because there was no "govt regulation covering KYC or AML." (Hayes PSR ¶ 16). BitMEX made a deliberate choice not to have KYC, and advertised this fact to its users. In November 2014, Hayes wrote to Delo that BitMEX would not do any KYC, saying "Basically just valid email address until we feel significant pressure to do otherwise." In about 2015, the Company's website advertised that "No real name or other advanced verification is required on BitMEX." (Hayes PSR ¶ 18). In a February 2017 blog post, Hayes wrote that "KYC and AML violations are used by governments worldwide to harass companies." <https://blog.bitmex.com/lockdown/> (accessed September 18, 2024).

In September 2015, the CFTC issued public enforcement orders conveying the CFTC's view that cryptocurrency was a commodity under the law. As they admitted at their guilty pleas, the Founders all understood that as a result, BitMEX's business model meant that if BitMEX continued to operate in the U.S., it had to comply with the AML and KYC rules. Rather than complying with these regulations, however, the Founders and Dwyer took steps to make it appear as if BitMEX was not operating in the United States, while continuing to conduct business in the United States and serve U.S. customers. Specifically, BitMEX placed a banner on its website and amended its terms of service to state that U.S. customers could not set up an account. It also implemented a block on new customers registering with a U.S.-based Internet Protocol ("IP") Address. (Hayes PSR ¶ 17).

These measures were pretextual. An obvious indication that BitMEX had no interest in actually preventing U.S. users from using the platform is that the Company knew that it already had a significant number of U.S. users in September 2015 and yet it did not remove them. (Hayes PSR ¶ 24). The new procedures were only applied to new users, not existing users. And even as to new users, BitMEX's Founders knew that the Company's supposed controls on U.S. customers were ineffective. BitMEX freely permitted users to trade on the platform with U.S. IP addresses. Rather than bar such addresses, BitMEX only ran a single IP address check when new users created accounts, making this purported control trivially easy to evade. (Hayes PSR ¶¶ 29-32). And even in the cases when a user's account was closed because it had been flagged as from the United States, the same user could still open a new account, using the exact same email address as the closed account. During its investigation, the Government identified multiple such users who did precisely that and then continued to freely operate on BitMEX. Finally, the Founders also

personally intervened to allow some prominent users personally known to them as U.S. persons to access and trade on BitMEX openly. (Hayes PSR ¶¶ 17, 24-27).

BitMEX had a clear financial motive not to implement effective measures to prevent U.S. users. The U.S. was a major market for crypto trading, and the Company's growth was driven in large part by its U.S. users. As late as July 2017, nearly two years after claiming to have banned U.S. users, the three Founders received a report from Greg Dwyer, who was BitMEX's first employee and also pleaded guilty for his role in the Company's BSA violations, that showed that the "United States remains the most popular country by visits and average number of active users per day." (Hayes PSR ¶ 21). Subsequent monthly revenue reports continued to show the presence of U.S. users on BitMEX. (Hayes PSR ¶ 22). In recognition of the importance of its U.S. customer base, BitMEX knowingly marketed itself to U.S. customers in numerous ways: for example, through its Affiliate Referral Program, BitMEX incentivized known U.S. customers to recruit new users, even though that had the effect of causing even more U.S. users to join the platform. (Hayes PSR ¶¶ 33-35). The Company executed a high-profile marketing stunt at a New York cryptocurrency event in May 2018, at which Hayes personally appeared with three Lamborghinis in midtown Manhattan.² Hayes also appeared frequently on U.S. television shows and discussed BitMEX, knowing that his appearances would mostly target U.S. users. At no point, however, did BitMEX implement any AML or KYC program. BitMEX continued to market itself to U.S. persons and knowingly provided services to large numbers of U.S. customers for more than five years after the Company knew that doing so required it to implement an AML/KYC program.³

² Hayes posted a photo of this event on his Twitter account in May 2018, and incredibly, has still not deleted the Tweet. See <https://x.com/CryptoHayes/status/996074905782423552> (visited September 18, 2024).

³ In its sentencing submission, BitMEX attempts to defend its procedures by claiming that its controls turned away more than \$100 million in revenue from U.S. users. (Def. Mem., at 6-7). But the source it cites for that proposition is an expert disclosure filed by Ben DeLo in advance of his criminal trial, and then included as an exhibit to his sentencing submission. The Government filed a motion to preclude that testimony that showed that the disclosure was riddled with errors and did not appear to be supported by the data on which it purportedly relied. *U.S. v. Hayes*, Dkt. 280, at

For years the Founders misrepresented BitMEX's U.S. presence. When an associate asked Hayes if BitMEX would be affected by CFTC enforcement activity in March 2016, Hayes falsely told him that BitMEX did not have a problem because "we don't allow US residents," and a few months later responded to a similar inquiry by stating falsely that "BitMEX openly does not server [sic] US customers. They are not allowed to enter the platform. We block all US IP addresses." (Hayes PSR ¶ 36). Hayes made the same false claim to a Wall Street Journal reporter the following year, stating "Due to CFTC regulations, BitMEX does not service Americans." (Hayes PSR ¶ 37). He made these false claims despite knowing that the Company was in fact allowing U.S. users to trade on the platform, and therefore was required to comply with these regulations.

In addition to servicing U.S. customers, BitMEX conducted business in the United States through employees and offices located in the U.S. From at least the spring of 2017 up to and including at least in or about January 2020, BitMEX acted through ABS Global, a Delaware-based subsidiary which operated BitMEX's technical operations including the front-end of the website and its popular API. In 2018 and part of 2019, BitMEX also had customer support staff stationed in the U.S., who responded directly to customers. Indeed, one of the primary reasons that BitMEX had U.S.-based staff was to ensure that there was adequate support coverage during U.S. business hours to appeal to the Company's large number of U.S. customers. The Company had an office in San Francisco for most of the relevant period, which had over 50 employees, and an office in New York through at least early 2019. One of the Founders, Sam Reed, also worked for the Company from the U.S. throughout the relevant period, including from his homes in Wisconsin and Massachusetts.

15-21. The Government submits that this figure is unreliable. In any event, even if it were true that the company's procedures had reduced its revenue by preventing some U.S. users from using the platform, that would not change the fact that the company knew the procedures were generally ineffective and that it was still earning substantial revenue from U.S. users.

As a result of the Company's total lack of AML/KYC, BitMEX not surprisingly became a platform for money laundering. In May 2018, Hayes specifically authorized the withdrawal of what he was told were "stolen bitcoins" from a user account. (Hayes PSR ¶¶ 43-44). The Company also allowed customers from sanctioned jurisdictions to trade openly through at least October 2017: indeed, Hayes and Delo authorized traders from Iran to continue trading in that period, and even after sanctioned jurisdictions were restricted, internal reports showed that customers from those jurisdictions continued to trade on the platform through at least as of April 2018, and Delo knew that their sanctions controls could be bypassed by at least as of November 2018. (Hayes PSR ¶¶ 45-46). And in addition to those issues, the Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") concluded that BitMEX had conducted at least \$209 million worth of transactions with known darknet markets and unregistered money services businesses providing mixing services. In August 2021, BitMEX settled the FinCEN enforcement action and did not admit or deny the regulator's finding. As part of its settlement with FinCEN, however, BitMEX filed hundreds of suspicious activity reports, which recognized at least \$80 million of suspicious funds had been transferred through BitMEX.

During the period of the offense conduct, when BitMEX was serving U.S. users yet intentionally choosing not to comply with its obligations under U.S. law, BitMEX became one of the most popular cryptocurrency derivatives exchanges, which allowed the Founders to profit handsomely. It is the Government's understanding that each Founder withdrew between \$100 million and \$150 million in dividend payments from the Company over the period of 2014 to September 2020. And the paper value of BitMEX was many times higher than that: according to Company records, it earned approximately \$1.355 billion in revenue during the charged time period, and the Founders claimed to be billionaires based on their ownership stakes in BitMEX.

BitMEX also made false statements to a foreign bank, which it knew would be relayed to U.S. banks in order to transfer tens of millions of dollars as part of BitMEX's operations. Through the time period from at least 2016 through 2018, Hayes, Delo, Dwyer and others at BitMEX made false statements to the Hong Kong branch of HSBC. (Hayes PSR ¶ 47). The false statements concerned the nature of the business and the ownership of a BitMEX affiliate, Shine Effort Limited (Shine Effort), and were designed to allow BitMEX to obtain bank and trading accounts that it needed to conduct its operations but otherwise could not maintain without deceiving the bank. These lies were brazen: over the course of months and on numerous separate occasions, in at least September 2015, April 2017, August 2017, and December 2017, Delo, Hayes and others lied to HSBC that Shine Effort was a real business uninvolved with cryptocurrency, rather than a wholly owned subsidiary of an unlicensed cryptocurrency exchange. Hayes, Delo, and Dwyer even doctored internal BitMEX documents to submit them to HSBC as purportedly describing the business activities of Shine Effort. (Hayes PSR ¶¶ 48-53).

PROCEDURAL HISTORY

On October 1, 2020, the indictment against the three Founders and Dwyer was unsealed. All four defendants entered guilty pleas shortly before their trial was scheduled in 2022. The Information charging BitMEX with violating the BSA was filed on July 10, 2024, and the Company entered a guilty plea to the Information on that date.

In its sentencing submission, BitMEX suggests that it was only charged because the Government was “not happy with the sentences imposed” on the Founders, and that the Government wants a “pound of flesh” because it is “dissatisfied.” (Def. Mem. at 3). Those accusations are incorrect and unfounded. The Government had a call with counsel for BitMEX in October 2020, after the indictment against the Founders and Dwyer was unsealed. In that initial

call, the Government communicated to counsel that it would consider a disposition with the Company after the cases against the individuals were resolved.⁴ Consideration of a corporate disposition on its own merits is not unusual and was appropriate in this case. It is DOJ policy that “Corporations should not be treated leniently because of their artificial nature nor should they be subject to harsher treatment.” Justice Manual, U.S. Department of Justice, Section 9-28.200.

The timing of these resolutions vary case by case, as appropriately dictated by the evidence, operational considerations, and the nature of the case. In some cases, the Department resolves with companies in advance of individual prosecutions, sometimes simultaneously and sometimes after. It is in no way inappropriate to wait to resolve the criminal case against the Company until after the criminal culpability of individuals in corporate management is determined, as happened here. Indeed, official DOJ policy states that prosecutors should consider a number of factors in reaching a decision as to the proper treatment of a corporate target, with one of the factors being “the pervasiveness of wrongdoing within the corporation, including the complicity in, or the condoning of, the wrongdoing by individuals in corporate management.” Justice Manual, U.S. Department of Justice, Section 9-28.300.

Thus, there was nothing unusual, and certainly nothing surprising to BitMEX’s counsel, about the fact that the Government reengaged with BitMEX counsel regarding a potential disposition with the Company after the Founders had entered their guilty pleas. The relevant

⁴ After reviewing BitMex’s sentencing submission, the Government reviewed its own contemporaneous notes of its telephone calls with BitMEX counsel. During an initial telephone call, which occurred on October 2, 2020, the Government said, in sum and substance, that it was focusing on the individual defendants and then would address the company’s criminal liability. In that telephone call, defense counsel for BitMEX raised providing a Filip factors presentation and the Government informed BitMEX counsel that it was not time sensitive that the presentation occur but that the Government would be happy to hear from BitMEX counsel on these issues in the future. At bottom, defendant’s claim that the Government is only seeking monetary penalties against BitMEX because of dissatisfaction with the sentences imposed on individual defendants is based on pure self-serving speculation about the Government’s intentions and motives.

question for the Court is the appropriate penalty for the Company, based on the seriousness of its conduct, the gain it reaped from the offense, and the other sentencing factors.

DISCUSSION

The Government respectfully submits that the United States Sentencing Guidelines range for the appropriate fine is a range of \$223 million to \$428 million, and that the appropriate sentence is at the high end of the Guidelines range, for a total sentence of \$428 million.

I. Application of the Sentencing Guidelines

To calculate the appropriate sentence for a corporation, the United States Sentencing Guidelines (“U.S.S.G.” or “Guidelines”) set forth a multi-step process. First the Court should calculate the base fine amount, which in this case is the amount of the Company’s gain from the offense. U.S.S.G. § 8C2.4. Second, the Court should calculate the culpability score based on U.S.S.G. § 8C2.5, which is used to determine the appropriate multiplier in U.S.S.G. § 8C2.6. The multiplier is multiplied by the base fine to generate a sentencing guidelines range, U.S.S.G. § 8C2.7, and the Court considers where within this range the fine should be set, U.S.S.G. § 8C2.8. Third, the Court shall then add to the fine the gain to the company, less any remedial payments the company has made, as disgorgement. U.S.S.G. § 8C2.9. Finally, because BitMEX was a closely held company, the Court should offset from the fine any fine amounts paid by the Founders. U.S.S.G. § 8C3.4.

A. Step One: Calculating the Gain from the Offense

1. A Conservative Estimate of the Company’s Gain is \$128 Million

The first step is to calculate the gain from the offense, which serves as the base fine level in this case pursuant to U.S.S.G. § 8C2.4(a)(1). Under the Guidelines, pecuniary gain is defined as “additional before-tax profit to the defendant resulting from the relevant conduct of the offense. Gain can result from either additional revenue or cost savings.” U.S.S.G. § 8A1.2, Application

Note 3(H). Thus, the question is what “additional revenue” or “cost savings” resulted from the offense conduct.

There are three reasonable approaches for calculating the revenue generated from the offense: (1) the revenue the Company earned while operating in the United States; (2) the revenue the Company earned from U.S. users; or (3) the revenue the Company earned from its willful decision to eschew an AML program. For the reasons described below, the Government respectfully submits that the second approach—a fine based on the Company’s revenue attributable to its U.S. customers—is a conservative approach that can be calculated with reasonable accuracy, and is therefore the most appropriate method to estimate the pecuniary gain from the offense. However, the Government will discuss all three approaches here.

As to the first approach, BitMEX plainly conducted business in the United States throughout the charged time period. The Commodity Exchange Act applies to all entities that “conduct any office or business in the United States.” 7 U.S.C. § 6. BitMEX was continuously physically present in this country because a significant portion of its workforce, including Founder and senior executive Sam Reed and dozens of Company employees, worked for the Company from the United States, and this is where it conducted essential elements of its business that applied to all trading activity on the platform. Because the Company had a permanent physical presence in the United States during the entirety of the relevant period, it was required to register with the CEA and to have a fully compliant AML and KYC program not only for its U.S. users, but for all of its users, and yet it did not implement any such program. Under a straightforward reading of the statute, the gain from the offense is the Company’s entire revenue from its non-compliant ongoing operations in this country. That calculation would result in a base offense level of \$1.355 billion.

The second approach for calculating the pecuniary gain—which the Government submits is the correct method to apply here—would be to base gain only on the revenue the Company earned from its U.S.-based *customers* (rather than its U.S.-based operations more broadly). This is the metric proposed by BitMEX itself, but its sentencing submission does not actually calculate this amount. (Def. Mem. at 15).

In January 2020, during the relevant period, as the Company was responding to the Government’s investigatory subpoena and requests from the CFTC, BitMEX itself calculated that 9.51% of its users who had ever traded on the platform were attributable to the U.S. The percentage of users from the U.S. is not a perfect proxy for the percentage of revenue attributable to U.S. users, but it is likely that the revenue attributable to U.S. users is higher than 9.51%. This is because BitMEX’s U.S. users included some of its most highly active traders from whom BitMEX earned substantial fees, including high-profile U.S.-based crypto trading firms known to trade in huge volumes. In addition, internal Company documents showed that the United States was the Company’s single largest country by number of active users for at least substantial portions of the charged time period. (Hayes PSR ¶ 21). Thus, a fair but conservative estimate, based on the Company’s own numbers, would indicate that at least 9.51% of the Company’s revenues were attributable to its U.S. users. As noted above, BitMEX had revenues of approximately \$1.355 billion during the charged period. Thus, if the pecuniary gain is calculated based on revenue attributable to U.S. users, then 9.51% of those revenues, or \$128.385 million, would be the pecuniary gain, and the base fine amount under the Guidelines.

In its sentencing submission, BitMEX challenges this calculation, asserting that “the Company’s user data does not map to revenue.” (Def. Mem. at 19). But tellingly, BitMEX has made no attempt to calculate an alternative number, despite the fact that the Company would

presumably be uniquely able to produce granular user and transaction data to more precisely estimate the revenue attributable to U.S. users if it thought such a calculation would be to its advantage. The Guidelines do not demand scientific precision. Here, as in other areas of the Guidelines, the Court need only determine a “reasonable estimate” of the gain from the offense. *Cf.* U.S.S.G. § 2B1.1 cmt. n. 3(C). An estimate of the percentage of revenue attributable to U.S. users based on the percentage of users from the U.S. is a reasonable way to calculate the gain to the Company. *See id.* (for purposes of U.S.S.G. § 2B1.1, the “estimate of the loss shall be based on available information,” considering what is “appropriate and practicable under the circumstances,” and acceptable methods include “the approximate number of victims multiplied by the average loss to each victim”). As noted, this number is almost certainly an underestimate given the other evidence of the significance of U.S. users to the platform.

The third potential metric for calculating pecuniary gain would be to attempt to estimate the amount of additional revenue the Company derived from its failure to implement a KYC/AML program. However, this metric is difficult to calculate with precision because it would be based on attempting to estimate how many users opened accounts with BitMEX specifically because they valued BitMEX’s lack of BSA controls. That said, the Company built itself as a no-KYC platform, explicitly marketing itself as an anonymous way to transact in cryptocurrency derivatives and even denigrating financial institutions that complied with the law. Thus, it is reasonable to posit that at least a substantial portion of the Company’s success and thus revenue during the relevant period was derived from the criminal activity. Support for this can be seen in the fact that BitMEX itself acknowledged that it “lost users and volume” after implementing certain KYC procedures in 2020. <https://blog.bitmex.com/what-weve-learned-six-months-after-becoming-the-largest-fully-verified-derivatives-exchange/>. Indeed, revenue in 2019, the last full year in which BitMEX had

no KYC procedures, was \$481 million, while revenue in 2021, the first full year in which BitMEX had KYC procedures, was \$264 million, which represents a drop of more than 40%. Even if there may have been other factors that contributed to this decline in revenue, these numbers indicate that the gain in revenue to BitMEX from marketing itself as a non-KYC exchange may have been more than a third of its total revenue, which would result in a calculation in excess of \$450 million.

Ultimately, the Government submits that the most conservative of these three methods, and the method that most readily yields an ascertainable number, is to use the second approach and calculate the gain based on the revenue attributable to U.S. users, that is, \$128.385 million. This was the number calculated by the Probation Office in the initial draft of the PSR, and even with notice of this number and the basis for it, the Company's sentencing submission provided no basis for any alternative calculation.

2. The Government Did Not Stipulate to Any Different Gain Amount

Instead of actually proposing a methodology for calculating the gain from the offense, the Company's only argument about its gain from the offense is to claim that the Government has somehow "stipulated" that the gain was \$30 million through its plea agreements with the Founders. That argument is contrary to the facts and the law.

First, as a factual matter, the fine amount in the plea agreement was based on the amount that the Government understood each defendant individually earned in dividends from BitMEX during the charged time period. The text of the plea agreements reflects this, as each agreement refers to "the pecuniary gain derived by the defendant from the offense," and says nothing that would indicate that the fine was also meant to capture how much gain BitMEX derived from the offense. At the time the plea agreements were negotiated, the Government's understanding was that each Founder had received around \$100 million in dividends during the charged time period,

so the appropriate individual fine was approximately 10% of that number, or \$10 million.⁵ The 10% number was based on the same methodology proposed by the Government here, the rough percentage of BitMEX users who were in the United States. As the Government explained in its sentencing submission for Hayes, the \$10 million fine was a “reasonable if conservative approximation of the direct pecuniary gain from the offense,” *i.e.*, the amount of actual money he received from BitMEX that was attributable to the offense conduct, but the fine expressly did “not capture the unquantifiable indirect value,” *i.e.*, the increase in value to BitMEX from the offense conduct. *United States v. Hayes*, 20 Cr. 500 (JGK), Dkt. No. 334, at 16. The Company cannot point to any statement by the Government that ever suggested the individual fines reflected the overall gain to the Company from the offense.

It was the Government’s intention, as expressed to BitMEX’s counsel from the outset, to reach a charging decision with respect to the Company separately from the Founders. The appropriate fine for BitMEX must be based on the gain that it reaped from the offense, which is a separate and greater number than the dividend payments that were made to the individual defendants during the course of the scheme.

BitMEX’s argument is also contrary to the law. Even if it were the case that the Government had reached a plea agreement with an individual defendant that purported to set a value for the total gain to BitMEX from the offense (and it plainly did not), that would not be binding in this case. BitMEX is not a party to any plea agreement. Nor does it claim that the plea agreements designate BitMEX as a third-party beneficiary. Any such argument would fail. As an initial matter, it is doubtful that a plea agreement even can confer enforceable rights on a third party. *See Santobello v. United States*, No. 94 Cr. 119 (RPP), 1998 WL 113950, at *3 (S.D.N.Y.

⁵ The Government has since learned that the Founders likely received as much as \$150 million in dividends during the charged time period, which would mean their individual fines were low.

Mar. 13, 1998) (“Even if Santobello could establish the existence of plea agreements between the Government and his co-defendants, there is little known authority that would allow him to enforce the agreements as a third party beneficiary.”). And even if a plea agreement could create such enforceable rights, BitMEX would have to demonstrate that the parties intended the agreement to confer third-party benefits on it. *E.g., Conway v. Icahn & Co., Inc.*, 16 F.3d 504, 509 (2d Cir. 1994). There is no evidence that the parties reached such an unusual agreement in this case. Rather, the Government agreed with the individual defendants to an individual fine amount based on the actual money they personally received during the offense, without reference to the total gain to the Company.

B. Step Two: The Culpability Score and Multiplier

After determining the gain amount, the next step in the analysis is to calculate the Company’s Culpability Score. Under U.S.S.G. § 8C2.5(a), the Culpability Score begins at 5. Then, according to U.S.S.G. 8C2.5(b)(3), 3 levels are added because the Company had more than 200 employees, and as described above, Company executives participated in the offense.

In its sentencing submission, the Company asserts that only a 2-level increase is warranted because it claims that it “has never had more than 200 employees.” (Def. Mem. at 19). The Company does not cite anything for that claim, and it produced a document to the CFTC that indicated otherwise. In February 2019, BitMEX produced a list of all users with access to its internal Slack space at the time, which listed 209 separate individual user identifications. (BMX-CFTC-00002944). As far as the Government is aware, only BitMEX employees had access to the Slack space, meaning that it had approximately 200 employees at that time. And the Company almost certainly grew between early 2019 and October 2020, when the Indictment was unsealed.

Press reports from after the Indictment suggest that BitMEX ultimately reached at least around 300 employees, although it is unclear when its headcount peaked.⁶

Moreover, in the initial draft of the PSR, the Probation Office concluded that the Company's "headcount" surpassed 200 personnel in May 2020, including contractors, and the Company did not object to that number. Instead, it argued to Probation that contractors should not be included in the employee count for Guidelines purposes. But the purpose of this Guideline is to calibrate the appropriate penalty to the size of the business; for this purpose, it is irrelevant whether a company conducts its operations through formal employees or through contractors who are functionally employed by the company. The Government therefore submits that, in interpreting the word "employee" in this Guideline, the question should be whether these personnel were under the direction of the Company and performing Company functions as their regular employment, as they were in this case as part of the Company's own "headcount." This interpretation is consistent with the interpretation of "employee" in other areas of the law. *See, e.g., Anthony v. Nw. Mut. Life Ins. Co.*, 130 F. Supp. 3d 644, 652 (N.D.N.Y. 2015) (Sarbanes-Oxley protections for whistleblower employees also apply to "a contractor employee [who] is functionally acting as an employee of a public company"). Thus, even if it were necessary to include contractor employees to reach the 200-employee threshold, the 3-level enhancement is warranted.

Next, the Court should consider whether to reduce the Culpability Score pursuant to U.S.S.G. § 8C2.5(g). BitMEX acknowledges that it is not entitled to a two or three-level reduction, but argues for a one-level reduction pursuant to § 8C2.5(g)(3). (Def. Mem. at 17). To be sure, the Company entered a guilty plea, which "ordinarily" suffices to show acceptance of responsibility

⁶ See TechCrunch, "BitMEX Crypto Exchange Lays Off a Quarter of Staff After Failed Acquisition," April 4, 2022, available at <https://techcrunch.com/2022/04/04/bitmex-crypto-exchange-lays-off-a-quarter-of-staff-after-failed-acquisition/> (accessed September 19, 2024) ("Derivatives-focused crypto exchange BitMEX has laid off about 75 employees, or a quarter of the company's staff ...").

for the one-point reduction. U.S.S.G. § 8C2.5 cmt. n. 14. However, the Government submits that this is not the ordinary case. BitMEX did not “clearly demonstrate[] recognition and affirmative acceptance of responsibility for its criminal conduct”; rather, BitMEX consistently argued to the Government that it had erroneously indicted the Founders, and that no willful BSA violation had been committed by the Company, maintaining these denials until after the Founders had pleaded guilty. It was only then, when BitMEX clearly had no defense, was guilty by operation of law due to the guilty pleas of its Founders and executives, and would only have been wasting its own resources to insist on a pro forma trial, that BitMEX indicated any willingness to plead guilty. Thus, the Government submits that this one-point reduction is unwarranted and the Culpability Score is 8.

Under U.S.S.G. § 8C2.6, a Culpability Score of 8 leads to a multiplier range of 1.6 to 3.2. Applying that multiplier to the gain amount results in a Guidelines fine range of \$205 million to \$410 million.⁷

The next step is for the Court to determine the fine within this range applying the factors set forth in U.S.S.G. § 8C2.8. For the reasons discussed below, the Government submits that a sentence at the high end of this range is warranted. The conduct was willful, it went on for a period of five years, and it was perpetrated at the highest levels of the Company. Thus, the applicable fine should be approximately \$410 million.

C. Steps Three and Four: Disgorgement and Offset

The next step is to include disgorgement, under which the Court “shall add to the fine” the amount of gain to the organization, but should reduce this disgorgement amount by anything that

⁷ If the Court were to agree with BitMEX that it is entitled to a one-point reduction for acceptance of responsibility, the Culpability Score would be 7, the multiplier would be 1.4 to 2.8, and this range would be \$179 million to \$359 million. If the Court were also to determine that BitMEX had fewer than 200 employees, the Culpability Score would be 6, the multiplier would be 1.2 to 2.4, and this range would be \$154 million to \$308 million.

has been “paid as restitution or by way of other remedial measures.” U.S.S.G. § 8C2.9. Here, the gain to BitMEX is \$128 million, but it has paid \$80 million to settle its cases with the CFTC and FinCEN. Thus, under U.S.S.G. § 8C2.9, the Court should add \$48 million to the fine, resulting in a total fine of \$458 million. In its sentencing submission, BitMEX suggests that the \$80 million it paid in civil fines should be credited against the Guidelines range rather than against the disgorgement. (Def. Mem. at 18). BitMEX cites no authority for that proposition, which is contrary to the text of U.S.S.G. § 8C2.9, which BitMEX does not even cite in its sentencing submission. Section 8C2.9 establishes that the civil fines are offset against the amount of disgorgement that is added to the Guidelines fine range, not against the fine range itself.

Finally, under U.S.S.G. § 8C3.4, the Court may offset the fine to reflect the amount paid by the Founders, given that BitMEX was and remains a closely held corporation. Reducing by \$30 million, the final fine number called for by the Guidelines is \$428 million if the Court agrees with the Government that a sentence at the high end of the range is warranted. The full Guidelines range is \$223 to \$428 million.⁸

II. The Nature, Circumstances, and Seriousness of the Offense

The nature of the offense counsels in favor of a sentence at the higher end of the Guidelines range. The BSA is designed to safeguard the financial system, both in the United States and around the world, from illicit use, and to combat money laundering. Financial institutions are required to implement AML programs so that the institutions do not foster criminal activity or lead to the diversion of victim funds. Cryptocurrency compounds the need for such programs because of the technology’s pseudonymity; without KYC and AML, a user of cryptocurrency could evade law enforcement by hiding behind the string of numbers describing their wallet address.

⁸ With a Culpability Score of 7, this range would be \$197 to \$377 million. With a Culpability Score of 6, this range would be \$172 million to \$326 million.

By operating without an AML program, BitMEX created a significant platform for cryptocurrency users to do exactly that. Due to BitMEX's criminal conduct, the full scope of the illegal behavior that BitMEX enabled cannot be precisely estimated. It is noteworthy, however, that FinCEN identified \$200 million in suspicious transactions. Similarly, the Company's refusal to implement a full KYC and AML program meant that it was more likely that BitMEX would allow sanctioned parties to trade, which they did. That sanctions evasion carries substantial costs to the U.S. financial system and U.S. national security interests.

Nor was this a crime of simple inadvertence. BitMEX's Founders knew for years that the Company was required to have KYC and AML programs but willfully permitted users to transact anonymously with no controls, and did so despite repeated warnings from law enforcement around the world about suspicious activities on the platform. To be clear, BitMEX did not simply have an inadequate AML program. It did not implement any AML program at all, and its failure to implement an AML program meant that it was harder for law enforcement to identify criminal activity and track victim funds.

In its sentencing submission, the Company downplays the seriousness of the offense by citing purported controls it put in place to prevent U.S. users. But as the Company's Founders admitted, they knew those controls were ineffective. Moreover, it is noteworthy that the only significant controls mentioned by BitMEX were implemented in late 2018, after the CFTC's investigation into BitMEX became overt. (Def. Mem. at 6). BitMEX claims that it lost potential revenue from U.S. users as a result of its controls, but as noted above in footnote 3, that claim is based on a highly unreliable pretrial expert disclosure and should not be credited. And even if it were true that BitMEX could have earned even more unlawful revenue, it would not follow that it should receive leniency for the unlawful revenue that it did earn. The Company's extensive

marketing to U.S. users, its maintenance of customer-support staff in the United States, and its own internal reports showing that the U.S. was one of its top sources of users, all indicate that the U.S. market was a key part of BitMEX's financial success.

BitMEX also argues that the Court should not consider its conduct in making misrepresentations to a Hong Kong-based affiliate of HSBC, which enabled it to make U.S. dollar transactions to support its business. BitMEX argues that this conduct is irrelevant because (in the Company's view) it is not a chargeable criminal offense in the United States. (Def. Mem. at 24). But that misses the point. Regardless of whether the Government could charge BitMEX with bank fraud or some other offense based on this conduct, the conduct itself is relevant in considering the overall seriousness of BitMEX's offense. The picture BitMEX is seeking to present to the Court is of a corporate "good citizen" that merely committed a regulatory violation. Its deliberate lies to a financial institution are just one additional piece of evidence that such a picture is decidedly false.

BitMEX also argues that its post-enforcement efforts to comply with the law by implementing steps to ensure that it does not have U.S. users indicate that a significant financial penalty is unwarranted. (Def. Mem. at 11-14). There are at least two reasons that is wrong. First, the Company was required to take those steps as part of a settlement with FinCEN, representing the bare minimum it needed to do to be in compliance with U.S. law. That is, these are steps that the Company had been legally required to implement from the beginning. While the Guidelines recognize that corporations may in some cases receive credit for self-reporting and fixing their legal violations before Government enforcement, it would be inappropriate to give a corporation credit for fixing its violations only after it is caught and subjected to a costly enforcement action. Compliance with the law is expected of all corporate actors—it is not an exceptional act that

warrants relief from the consequences of criminal conduct. Second, BitMEX already reaped a substantial benefit from implementing these measures, as FinCEN agreed to forgo \$20 million in fines if BitMEX implemented them. There is no basis to give BitMEX additional credit when it has received exactly what it bargained for with FinCEN in exchange for putting these measures in place.

III. A Substantial Financial Penalty is Required to Afford General Deterrence and to Promote Respect for the Law

Next, a substantial financial penalty is required to afford general deterrence and to promote respect for the law.

BitMEX argues that the Government’s “prosecution and enforcement actions taken to date” have sufficiently deterred the Company and its Founders and promoted respect for the law in the “crypto industry.” (Def. Mem. at 20-23). In support of that argument, BitMEX primarily cites (1) press releases issued immediately after the announcement of the indictment against the BitMEX Founders in October 2020, including an October 2020 press release in which Binance’s CEO was quoted as describing the BitMEX charges as a “wake-up call” to the industry; and (2) statements of remorse made by the Founders during their 2022 sentencings. *See id.* Defense counsel is certainly correct that the indictment of the Founders in October 2020 was a significant milestone in BSA enforcement in the cryptocurrency industry. The indictment made plain to the industry that the AML and KYC violations long being committed by its participants were not only criminal but would be prosecuted. However, the deterrent value of the charges now brought against BitMEX will be realized only if the Company is faced with serious financial penalties that reflect the full scope of its corporate misconduct and the seriousness of the offense, as described above. Indeed, the notion that the 2020 charges against the Founders, or their 2022 sentencings, have sufficiently resulted in deterrence or respect for the law is belied by later events.

Even since the filing of the charges in this case in 2020, major cryptocurrency exchanges have continued to engage in flagrant regulatory and criminal violations and to be charged civilly and criminally in connection with those offenses. For example, Binance and its CEO were charged by the CFTC in March 2023 for AML and KYC-related violations that allegedly continued for years after the 2020 indictment against the Founders which, as noted above, was touted by Binance’s CEO as a “wake-up call” to the industry.⁹ Apparently not so. Not only was Binance undeterred by the charges against BitMEX’s Founders, but the company used its understanding of the significance of BitMEX’s case to alter its practices to further *hide* its ongoing AML and KYC failures. As alleged in the CFTC complaint, for example, Binance responded to the news of the BitMEX indictment by actively concealing U.S. user data, which from that point forward would be visible to “very few people” in the company. As part of a coordinated resolution with the CFTC, the DOJ, and FinCEN, Binance and its CEO later pleaded guilty to criminal BSA charges and related offenses. The company agreed to pay more than \$4 billion to resolve those charges.¹⁰ More recently, in March 2024, a grand jury sitting in this district brought an indictment against the cryptocurrency exchange Kucoin, and two of its founders, for allegedly engaging in materially similar BSA violations to BitMEX and its Founders.¹¹ In short, while the 2020 charges against the Founders put crypto companies on notice of the criminality of their conduct, the charges themselves were not sufficient to deter such conduct from continuing to occur or to promote respect for the law.

⁹ See CFTC Press Release No. 680-23, CFTC Charges Binance and its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange (Mar. 27, 2023), <https://www.cftc.gov/PressRoom/PressReleases/8680-23>.

¹⁰ See DOJ Press Release, Binance and CEO Plead Guilty to Federal Charges in \$4 B Resolution (Nov. 21, 2023), <https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution>.

¹¹ See DOJ Press Release, Prominent Global Cryptocurrency Exchange Kucoin and Two of Its Founders Criminally Charged with Bank Secrecy Act and Unlicensed Money Transmission Offenses (Mar. 26, 2024), <https://www.justice.gov/usao-sdny/pr/prominent-global-cryptocurrency-exchange-kucoin-and-two-its-founders-criminally>.

Notably, the mere fact that another company has been charged, while significant, does not by itself alter the cost-benefit analysis for cryptocurrency companies weighing whether to violate the law. There must be a financial penalty that communicates that the costs of lawbreaking exceed the benefits. It would undermine that message if BitMEX were ordered merely to repay its gains from the offense, rather than to be penalized in accordance with the formula recommended by the Sentencing Guidelines. And it would obliterate that message if BitMEX were actually allowed to escape without paying any financial penalty, as it proposes in its sentencing submission. Such a sentence would essentially telegraph to other similarly situated cryptocurrency exchanges that they can flagrantly violate the BSA by servicing U.S. customers without an adequate KYC/AML program, regardless of the resulting criminal and suspicious money flows they facilitate, reap financial gains from that behavior, and then retain a substantial portion of those gains even if they are apprehended. That cannot and should not be the financial calculus for other similarly situated cryptocurrency exchanges.

This Court can and should impose a sentence that sends a clear message to other cryptocurrency exchanges that the potential financial gain that can be reaped from servicing U.S. users without implementing a BSA-compliant program is not worth the resulting penalty. *United States v. Heffernan*, 43 F.3d 1144, 1149 (7th Cir. 1994) (Posner, J.) (“Considerations of (general) deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish, since both attributes go to increase the expected benefits of a crime and hence the punishment required to deter it.”); *see also United States v. Zukerman*, 897 F.3d 423, 429 (2d Cir. 2018) (citing *Heffernan*). Moreover, given that BitMEX’s BSA failures allowed for substantial money laundering to occur, as well as sanctions evasion, general deterrence is particularly important in this case.

For all of the foregoing reasons, a substantial financial penalty is necessary to serve the sentencing objectives of general deterrence and promoting respect for the law.

IV. Comparator Cases

A fine of approximately \$428 million, at the high end of the Guidelines range, is also in line with similar corporate resolutions in the Bank Secrecy Act and similar contexts. For instance, U.S. Bancorp entered into a deferred prosecution with the United States in 2018 for its violations of the BSA, and agreed to pay a \$528 million penalty. Importantly, this penalty was not a systemic failure like the conduct at issue here, but was instead based on the amount of funds which a single fraud perpetrator had transferred through the bank without it performing adequate anti-money laundering scrutiny. *United States v. \$453,000,000 in United States Currency*, 18 Civ. 1357 (AJN), Dkt. No. 1 (forfeiting the substitute *res* as “constitut[ing] proceeds of wire fraud, in violation of Title 18, United States Code, Section 1343, and property involved in money laundering, in violation of Title 18, United States Code, Section 1956”). If anything, the conduct here is more significant because it did not involve a single instance where the AML policy failed, but a complete failure to have any AML policy. Similarly, Commerzbank entered into a deferred prosecution agreement in 2015 for BSA and sanctions violations, and paid a \$1.45 billion penalty, including \$300 million for BSA-related conduct, including failure to file suspicious activity reports. *United States v. \$300,000,000 in United States Currency*, 15 Civ. 1825 (PGG), Dkt. No. 1, ¶¶ 13–14. Recently, cryptocurrency exchange Binance entered into a plea agreement with the Department of Justice and agreed to pay a fine of \$1.8 billion as well as billions more in forfeiture. *United States v. Binance*, 23 Cr. 178 (W.D. Wash.), Dkt. No. 23 ¶ 14(a). The higher penalty that Binance paid is warranted by the fact that it also pleaded guilty to sanctions violations and unlicensed money transmitting. But its conduct in failing to have an adequate AML policy was analogous to BitMEX’s conduct in this case, and formed a substantial part of the conduct for which the fine was

imposed. *Id.* ¶ 3(a). These prior corporate resolutions illustrate that a Guidelines fine in this case is well within the norm for similar conduct.

CONCLUSION

In light of the record, the Sentencing Guidelines, and the Section 3553(a) factors, the Government respectfully submits that a sentence at the high end of the Guidelines range is warranted. Accordingly, the Court should impose a fine of \$428 million.

Dated: New York, New York
September 20, 2024

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

By: s/ Thane Rehn
Jessica Greenwood
Thane Rehn
Assistant United States Attorneys
(212) 637-1090/2354